With reference to FIG. **24**, for example, a computer system has a high-level application environment (level L**4**). These applications invoke (call) operating system level (L**3**) processes to perform various system functions. The OS level (L**3**) processes in turn invoke lower-level Basic Input/Output System (BIOS) machine dependent instructions as required (level L**2**). Note that application level (L**4**) programs might be permitted to bypass the OS level (L**3**) and invoke BIOS level (L**2**) processes directly, thereby avoiding any OS level (L**3**) policy checking and enforcement.

As an example, an application (executing a level L**4**) program which wishes to open a particular named file would invoke an operating system "open" procedure for that named file. The OS determines the location of the file (using, for example, an internal map between file names and locations) and then invokes a lower level (L**2**) BIOS routine to perform the actual seek to the file and the open and read. However, the application program might be permitted to bypass the operating system's "open" process and invoke the BIOS routines directly.

It is desirable to implement the access control mechanisms of the present invention at a low level, preferably at or below the BIOS level (level L**1**). This prevents users from by-passing the access control mechanisms of the invention and thereby circumventing the rule enforcement.

Thus, a system for controlling access and distribution of digital property is provided. One skilled in the art will appreciate that the present invention can be practiced by other than the described embodiments, which are presented for purposes of illustration and not limitation, and the present invention is limited only by the claims that follow.

What is claimed is:

1. A method of distributing data, the method comprising:

protecting portions of the data; and

openly distributing the protected portions of the data, whereby

each and every access to an unprotected form of the protected portions of the data is limited in accordance with rules defining access rights to the data as enforced by an access mechanism, so that unauthorized access to the protected portions of the data is not to the unprotected form of the protected portions of the data.

2. A method as in claim **1**, wherein

the protecting of portions of the data comprises encrypting the portions of the data, whereby unauthorized access to the protected data is not to the un-encrypted form of the protected data.

3. A method as in claim **2**, wherein the encrypting of portions of the data encrypts the portions of the data with a data encrypting key, the data encrypting key having a corresponding data decrypting key, the method further comprising:

encrypting the data encrypting key.

4. A method as in claim **3**, further comprising:

providing a decrypting key corresponding to the key encrypting key.

5. A method as in claim **1**, wherein the data represent at least one of software, text, numbers, graphics, audio, and video.

6. A method as in claim **1**, wherein the rules indicate which users are allowed to access the protected portions of the data, the method further comprising

allowing the user access to the unprotected form of a protected portion of the data only if the rules indicate that the user is allowed to access that portion of the data.

7. A method as in claim **1** wherein the rules indicate distribution rights of the data, the method further comprising:

allowing distribution of the unprotected form of the protected data portions only in accordance with the distribution rights indicated in the rules.

8. A method as in claim **1**, wherein the rules indicate access control rights of the user, the method further comprising:

allowing the user to access the unprotected form of the protected data portions only in accordance with the access control rights indicated in the rules.

9. A method as in claim **8**, wherein the access control rights include at least one of:

local display rights,

printing rights,

copying rights,

execution rights,

transmission rights, and

modification rights.

10. A method as in claim **1**, wherein the rules indicate access control quantities, the method further comprising:

allowing access to the unprotected form of the protected data portions only in accordance with the access control quantities indicated in the rules.

11. A method as in claim **10**, wherein the access control quantities include at least one of:

a number of allowed read-accesses to the data;

an allowable size of a read-access to the data;

an expiration date of the data;

an intensity of accesses to the data;

an allowed level of accuracy and fidelity; and

an allowed resolution of access to the data.

12. A method as in claim **1**, wherein the rules indicate payment requirements, the method further comprising:

allowing access to the unprotected form of the protected data portions only if the payment requirements indicated in the rules are satisfied.

13. A method as in claim **1**, wherein the rules relate to at least one of:

characteristics of users;

characteristics of protected data; and

environmental characteristics.

14. A method as in claim **1** wherein the rules defining access rights include at least one internal rule built in the access mechanism.

15. A method as in claim **14** wherein the at least one internal rule cannot be made less restrictive by any other rules.

16. A method as in claim **14** wherein the access mechanism is contained in a stand-alone device.

17. A method as in claim **16** wherein the stand-alone device is selected from the group consisting of: a facsimile machine, a television, a VCR, a laser printer, a telephone, a laser disk player, and a computer system.

18. A method as in claim **1**,

wherein the access mechanism is contained in a stand-alone device selected from the group comprising: a facsimile machine, a television, a VCR, a laser printer, a telephone, a laser disk player, and a computer system; and

wherein the rules defining access rights include at least one internal rule built-in to the access mechanism; and